Notice of Allowability	Application No.	Applicant(s)	
	09/316,804	HIND ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *10/21/04*.

2. ☒ The allowed claim(s) is/are *2-4,6,8-10,12,14-16 and 18-22*.

3. ☒ The drawings filed on *5/21/1999* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Examiner's Statement of Reasons for Allowance

1. Claims 2-4,6,8-10,12,14-16,18-22 are allowed over prior art.

2. This action is in reply to applicant's correspondence of 21 October 2004.

3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

4. As per claims 2,6 prior art of record, Debry, U.S. Patent 6,314,521 B1, and Netscape ("Netscape") Communications Corp., "Netscape Certificate Server FAQ", 1997, fails to teach, alone, or in combination, of;

(claim 2) " A method for *initializing* a first *device distributed with an embedded radio* module *using a server*, said server *having an embedded radio module*, said method comprising the steps of:

sending an *inquiry* from said server *to said first device using said embedded radio modules*;

returning, from said first device, a *unique device identifier* of said first device, to said server;

creating, at said server, a *public key, private key pair for said first device*;

creating, at said server, a *device certificate* for said first device, said device certificate having

a unique hardware identifier associated with said first device and

a public key associated with said first device;

transmitting

said *private key*, and

said *device certificate*, and

a *public key of a Certificate Authority* which signed said device certificate, to said first device; and,

storing said private key in non-removable protected storage at said first device;

wherein said protected *storage is write-only storage able to perform computations involving previously-written data*." ;

(claim 6) "A method for initializing a first device distributed with an embedded radio module using a server, said server having an embedded radio module, said method comprising the steps of:

sending an inquiry from said server to said first device using said embedded radio modules;

creating at said first device, a public key, private key pair for said first device;

storing, at said first device, said private key in non-removable protected storage;

returning from said first device,

a unique device identifier and

said public key of said first device, to said server;

creating, at said server, a device certificate for said first device, said device certificate having

said device identifier and

said public key; and

transmitting

said device certificate and

a public key of a Certificate Authority which signed said device certificate to said first device;

wherein said protected storage is write-only storage able to perform computations involving previously-written data.";

5. The italicized above claim elements dealing with (for example; claim 1) " ... initializing ... device distributed with an embedded radio ... using a server, ... having an embedded radio module, ... inquiry ... to said first device using said embedded radio modules;... returning, ... unique device identifier ... public key, private key pair for said first device... device certificate ...transmitting ... private key, ... device certificate, ... public key of a Certificate Authority ...storing said private key ... storage is write-only storage able to perform computations involving previously-written data.. " serving to patently distinguish the invention from prior art. Specifically, while the use of private/public key pairs, the creation of associated digital certificate associated with a user or device, the sending of the certificate/public key over a communications channel (i.e., a wireless channel via the embedded radio modules), and the certificate verified for authenticity via a CA (with the devices concerned being wireless devices per se); is known in the prior art (i.e., see Hammond, J., et al, "Wireless Hotspot Deployment Guide", Intel Corp., Sept. 2004, www.intel.com/business/bss/infrastructure/wireless/deployment/hotspot.pdf), the sending of the *private key with the certificate across a wireless* (i.e., local between device and server), is

patently distinct in the art. Typically, the point of the certificate is subsequent transfer of the *public part* of the private/public key pair with the aid of the certificate structure/functionality.

As per the applicants arguments in the previous remarks in the Amendment (October 21, 2004), the examiner finds the applicant's arguments to be persuasive in that the 35 U.S.C. 112' rejection concerned with the embedded radio and device write only storage may be improper, allowing for the broadness in interpretation of the claim language.

Prior art of record specifically deals with standard use of private/public key pairs, the creation of associated digital certificate associated with a user or device, etc., in specific environments that typically do not encompass the localized communications environment involved with cryptographic functions and services associated with communications devices (i.e., provisioning a cell phone). There is nowhere implicitly or explicitly any mention of embedded radio environments used for certificate *with* private key transfer.

However, the claim language clearly associates the applicant's invention to the use with embedded radio based technologies per se, with the devices involved with the initializing subsequently storing the associated private key in non-removable, write only storage. This is in contrast to smartcard or other removable token based environments and technologies generally used for wireless provisioning, cryptographic parameter transfer/initializing.

6. Claims 14,18 and 8,12 deal with the software embodiment and system aspects, respectively, of the methods of claim 2.

7. Dependent claims 3,4,9,10,15,16, and 19-22 are allowable by virtue of their dependencies.

Conclusion

8. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100